KAZEROUNI LAW GROUP, APC
Abbas Kazerounian (SBN: 249203)
ak@kazlg.com
Mona Amini (SBN: 296829)
mona@kazlg.com
245 Fischer Avenue, Suite D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

ROBINSON CALCAGNIE, INC.
Daniel S. Robinson (SBN 244245)
drobinson@robinsonfirm.com
Michael W. Olson (SBN 312857)
molson@robinsonfirm.com
19 Corporate Plaza Drive
Newport Beach, California
Telephone: (949) 720-1288
Facsimile: (949) 720-1292

Attorneys for Plaintiff,
Faisal Moledina

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

FAISAL MOLEDINA, individually and on behalf of all others similarly situated, Plaintiff, vs. LIVE NATION ENTERTAINMENT, INC.; and TICKETMASTER L.L.C., Defendants.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

//

//

//

//

Plaintiff Faisal Moledina ("Plaintiff"), by and through their undersigned counsel, files this Class Action Complaint individually on behalf of themself and on behalf of all others similarly situated, against Defendants Live Nation Entertainment, Inc. ("Live Nation") and Ticketmaster L.L.C. ("Ticketmaster") (jointly as "Defendants"). Plaintiff bases the below allegations on personal information and belief, as well as the investigation of counsel, and states the following:

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and other similarly situated current and former Ticketmaster customers' (collectively defined herein as the "Class" or "Class Members") personally identifiable information ("PII"), including names, addresses, and credit card information (collectively, the "Private Information") from cybercriminals.

2. Pursuant the U.S. Securities and Exchange Commission (SEC) data breach disclosure rules, publicly owned companies operating in the U.S. must comply with a new set of rules requiring them to disclose "material" cyber incidents a Form 8-K report within 96 hours.

3. In a May 31, 2024 Form 8-K filing with the SEC, Ticketmaster's parent company, Live Nation, reported that on May 20, 2024, it "identified unauthorized activity within a third-party cloud database environment" which primarily contained data from its Ticketmaster L.L.C. subsidiary (the "Data Breach").[1] Live Nation further reported in its filing that "[o]n May 27, 2024, a criminal threat actor offered what it alleged to be Company user data for sale via the dark web." Upon detecting unauthorized activity, Live Nation began "working to mitigate risk to our users and the Company, and have notified and are cooperating with law enforcement" and stated it would also be notifying regulatory authorities and users with respect to

[1] https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm

KAZEROUNI LAW GROUP, APC

unauthorized access to personal information "as appropriate." Flippantly, Live Nation stated, "the incident has not had, and we do not believe it is reasonably likely to have, a material impact on our overall business operations or on our financial condition or results of operations." However, Live Nation further indicated that they "continue to evaluate the risks and our remediation efforts are ongoing."

4. The notorious ShinyHunters hacking group boasted regarding the Data Breach on the dark web, claiming to be in possession of 1.3 terabytes of data stolen by hackers from Ticketmaster, including but not limited to names, addresses, email addresses, telephone numbers, credit card information, belonging to 560 million Ticketmaster users; and offered to sell the data stolen in the Data Breach for $500,000.00.

5. According to threat intelligence and research group Vx-Underground, which claims it spoke with multiple individuals privy to and involved in the Data Breach, and analyzed a sample of the allegedly stolen data, the data exfiltrated in the Data Breach appeared to be authentic and included entries dating back to 2011, with the most recent ones being dated March 2024, and included data from the mid-2000's, and included full names, mail addresses, addresses, telephone numbers, credit card numbers, credit card type, authentication type, and all user financial transactions.[2]

6. By acquiring Plaintiff's and Class members' Private Information for their own pecuniary benefit, Defendants assumed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' Private Information against unauthorized access and disclosure.

7. The Data Breach was a direct and proximate result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols,

[2] https://x.com/vxunderground/status/1796063116574314642

KAZEROUNI LAW GROUP, APC

consistent with the industry standard, necessary to protect Private Information from the foreseeable threat of a cyberattack.

8. As a result of the Data Breach, and in light of their Private Information now being in the hands of cybercriminals, Plaintiff and the Class Members are, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. This substantial and imminent risk will continue indefinitely remain for their respective lifetimes.

9. As a result of Defendants' conduct, Plaintiff and the Class have and will be required to continue to undertake time-consuming and often costly efforts to mitigate the actual and potential harm caused by the Data Breach. This includes efforts to mitigate the Data Breach's exposure of their Private Information and PII, including by, among other things, placing freezes and setting alerts with credit reporting agencies, contacting financial institutions, closing, or modifying financial accounts, reviewing, and monitoring credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate records.

10. Armed with the Private Information accessed and exfiltrated in the Data Breach, the cybercriminals who carried out the Data Breach, as well as other unauthorized parties who obtained the Private Information as a result of the Data Breach, can and will commit a variety of crimes, including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, and using Class Members' financial information to make unauthorized and fraudulent transactions.

11. There has been no assurance offered by Defendants that all personal data or copies of data have been recovered or destroyed, or that it has adequately enhanced its data security practices sufficiently to avoid a similar breach of its network in the future.

12. Plaintiff therefore brings this Class Action seeking injunctive relief and

KAZEROUNI LAW GROUP, APC

damages against Defendants, individually and on behalf of all other persons whose Private Information was impacted by the Data Breach resulting from Defendants' inadequate data security procedures and practices.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005. Subject matter jurisdiction is proper because: (1) the amount in controversy in this class action exceeds five million dollars ($5,000,000), excluding interest and costs; (2) there are more than 100 Class members; (3) at least one member of the Class is diverse from the Defendants; and (4) the Defendants are not a government entity.

14. This Court has personal jurisdiction over Defendants because Defendants;' acts or omissions and false or misleading representations regarding the security of Plaintiff's and Class members' Private Information have impacted Plaintiff, who resides in this District; and Defendants each maintain a headquarters or principal place of business in Beverly Hills, California, and transact business from within this District.

15. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part events and injury giving rise to Plaintiff's claims occurred in or originated from this District and Defendants each maintain a headquarters or principal place of business in Beverly Hills, California, and transact business from within this District.

PARTIES

16. Plaintiff is and has been at all relevant times a citizen and resident of Los Angeles County, California. Plaintiff has been a customer of Ticketmaster for several years. Plaintiff provided his Private Information to Defendants, including his name, address, email address, telephone number, and credit card information, as required by Defendants in order to purchase or transfer tickets through Ticketmaster. Plaintiff reasonably relied upon Defendants to take reasonable steps to ensure that

KAZEROUNI LAW GROUP, APC

this information remained private, safe, and secure from breaches and cyberattacks.

17. Plaintiff is careful about sharing his sensitive Private Information. Plaintiff first learned of the Data Breach after hearing that hackers obtained information from Defendants in a Data Breach and were selling Ticketmaster customer data on the dark web. Upon receiving notice of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, reviewing his financial accounts and credit reports. Plaintiff has and is continuing to experience fear, stress, and frustration because Defendants allowed his Private Information to be accessed and taken by unauthorized parties who may have sold his Private Information on the dark web and may use that information for unknown nefarious purposes. Plaintiff has suffered actual injuries in the form of damages to and diminution in the value of his Private Information and PII—a form of intangible property entrusted to Defendants, which was compromised in and as a proximate result of the Data Breach. Plaintiff has suffered, and will continue to suffer, imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals for the remainder of his life.

18. Plaintiff has a continuing interest in ensuring that his Private Information, which remains within Defendants' possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

19. Defendant Live Nation is an American multinational entertainment company that was founded in 2010 following the merger of Live Nation and Ticketmaster that promotes, operates and manages ticket sales for live entertainment internationally. Live Nation is a corporation organized under the laws of Delaware with a corporate headquarters, or principal place of business, located in Beverly Hills, California.

20. Defendant Ticketmaster is an American ticket sales and distribution

KAZEROUNI LAW GROUP, APC

company that is a subsidiary of Live Nation following its merger with Live Nation in 2010. Ticketmaster is a limited liability company organized under the laws of the State of Virginia, with a corporate headquarters, or principal place of business, located in Beverly Hills, California.

FACTUAL BACKGROUND

A. Defendants Collected, Maintained, and Stored PII.

21. Prior to the Data Breach, Plaintiff and Class members provided their Private Information, including but not limited to names, email addresses, telephone numbers, credit card information, to Defendants in order to register for a Ticketmaster account or to make ticket-related transactions through Ticketmaster (*e.g.*, purchasing, selling, or transferring tickets) with the reasonable expectation that Defendants would take reasonable steps to ensure that this information remained private, safe, and secure from breaches and cyberattacks, which Defendants ultimately failed to do.

22. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

B. Defendants Knew They Needed to Protect Customers' Sensitive Private Information and Committed to Protecting their PII.

23. In affirming its privacy commitments[3] to Plaintiff and the Class members, Ticketmaster promised Plaintiff and the Class members, among other things, to keep their Private Information private; comply with industry standards all federal and state laws related to data security and the protection and maintenance of their Private Information with the following representations:

[3] https://privacy.ticketmaster.com/en/our-commitments

KAZEROUNI LAW GROUP, APC

> **Fair & Lawful**
> We comply with all applicable data protection laws and listen to your expectations when it comes to how your information is handled.
>
> **Security & Confidentiality**
> The security of our fans' information is a priority for us. We take all necessary security measures to protect personal information that's shared and stored with us.
>
> **Third Parties & Partners**
> We work with our partners to put on amazing live events and provide additional services that we think you'll love. We always ask them to maintain the same standards of privacy.
>
> **Storage & Retention**
> We store and use your data only as long as we need to, from complying with our legal obligations to making sure you know when your favorite artist is on tour.
>
> **Global Commitment**
> As an international company, no matter where you are located, our control framework is built around global data protection laws.
>
> **Accountability**
> Our global privacy office is staffed by a team of passionate privacy professionals who, in partnership with the business, deliver on our commitments, keeping our fans' information and their rights at the heart of what we do.

24. Ticketmaster's Privacy Policy also assured Plaintiff and the Class members, "We have security measures in place to protect your information" and "We have a global privacy team of trust and security professionals that ensure end-to-end protection of your personal information throughout the data lifecycle."[4]

25. Based on such policies and representations, Defendants knew they needed to protect the privacy and safeguard the sensitive Private Information and PII of its current and former customers, including Plaintiff and the Class members.

C. Defendants Failed to Comply with FTC Guidelines

26. In The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable

[4] https://privacy.ticketmaster.com/privacy-policy

KAZEROUNI LAW GROUP, APC

data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

27. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

28. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

29. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

KAZEROUNI LAW GROUP, APC

30. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

31. Defendants were at all times fully aware of Defendants' obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from its failure to do so.

32. Upon information and belief, the actors accessed and acquired substantial amounts of Plaintiff's and the Class's sensitive Private Information, including their PII. This data included sensitive personal information such as names, addresses, email addresses, telephone numbers, and credit card information.

33. Given that Defendants purposefully obtained and stored the Private Information, including PII, of Plaintiff and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendants were obligated to implement reasonable measures to prevent and detect cyberattacks. This includes measures recommended by the Federal Trade Commission ("FTC") and promoted by data security experts and other agencies. This obligation stems from the foreseeable risk of a data breach given that Defendants collected, stored, and had access to a swath of highly sensitive consumer records and data and, additionally, because other highly publicized data breaches at different institutions put Defendants on notice that the highly personal data they stored, or allowed other entities to store via a services contract or relationship, might be targeted by cybercriminals.

34. Despite the highly sensitive nature of the personal information Defendants obtained, created, and stored, and the prevalence of data breaches at financial institutions like Defendants or related businesses, Defendants inexplicably failed to implement and maintain reasonable and adequate security procedures and

KAZEROUNI LAW GROUP, APC

practices to safeguard the Private Information of Plaintiff and the Class. The Data Breach itself and information Defendants have disclosed about the breach to date, including the need to remediate Defendants' cybersecurity, the sensitive nature of the impacted data, and the fact that the data obtained in the Data Breach was already offered for sale on the dark web, collectively demonstrates Defendants failed to implement reasonable measures to prevent the Data Breach and the exposure of highly sensitive Private Information of Plaintiff and the Class members.

D. Defendants Failed to Comply with Industry Standards

35. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

36. Some industry best practices that should be implemented by businesses dealing with sensitive PII like Defendants include but are not limited to: education of all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

37. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

38. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security

KAZEROUNI LAW GROUP, APC

Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

39. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Exposure of PII and other Sensitive Private Information Created a Substantial Risk of Harm to Plaintiff and the Class

40. The personal and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves.

41. Upon information and belief, Plaintiff's and the Class members' sensitive Private Information and/or PII has been made available on the dark web as a result of the Data Breach.

42. Defendants' failure to reasonably safeguard Plaintiff's and the Class's Private Information has created a serious risk to Plaintiff and the Class, including both a short-term and long-term risk of identity theft and other fraud.

43. Identity theft occurs when someone uses another's personal and financial information such as that person's name, address, telephone number, email address, credit card information, and/or other information, without permission, to commit fraud or other crimes.

44. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[5]

45. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

46. Purchasers of PII use it to gain access to the victim's bank accounts,

[5] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com

KAZEROUNI LAW GROUP, APC

social media, credit cards, and tax details. This can result in the discovery and release of additional PII from the victim, as well as PII from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harms.

47. The FBI's Internet Crime Complaint (IC3) 2019 report estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help stop fraudulent transactions and mitigate losses.

48. The FTC has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour reiterated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[6]

49. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed or can be disposed of pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry tested and accepted methods;

(6) monitoring activity on networks to uncover unapproved activity;

[6] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable.

KAZEROUNI LAW GROUP, APC

(7) verifying that privacy and security features function properly;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[7]

50. The United States Cybersecurity & Infrastructure Security Agency ("CISA"), and other federal agencies, recommend similar and supplemental measures to prevent and detect cyberattacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

51. The FTC cautions businesses that failure to protect PII and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the fallout.[8] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Defendants failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

F. Defendants Breached Their Duty to Safeguard Plaintiff's and Class Members' Private Information

52. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols

---

[7] *Start With Security, A Guide for Business,* FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[8] Taking Charge, What to Do if Your Identity is Stolen, FTC, https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0014-identity-theft.pdf.

KAZEROUNI LAW GROUP, APC

adequately protected the Private Information of Plaintiff and Class members.

53. Defendants breached its obligations to Plaintiff and Class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customer and employee Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of customer and employee Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA; and

f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

54. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

55. Had Defendants remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class members' confidential Private Information.

56. Accordingly, Plaintiff's and Class members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and

KAZEROUNI LAW GROUP, APC

now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class members also lost the benefit of the bargain they made with the Defendants.

G. Defendants Should Have Known That Cybercriminals Target PII to Cary Out Fraud and Identity Theft

57. The FTC hosted a workshop to discuss "informational injuries," which are injuries that individuals like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[9] Exposure of highly sensitive personal information that an individual wishes to keep private may cause harm to that individual, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

58. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

59. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a

---

[9] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on April 10, 2024).

KAZEROUNI LAW GROUP, APC

form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

60. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

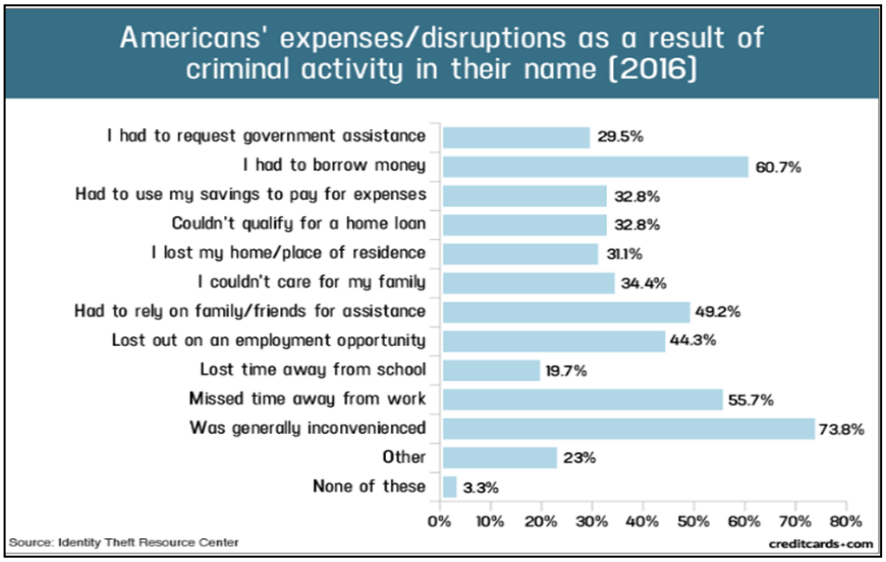
61. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

62. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[10] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

[10] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited April 10, 2024).

KAZEROUNI LAW GROUP, APC

63. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.



64. The ramifications of Defendants' failure to keep its customers' and employees' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

65. The value of PII is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

66. PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

67. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

KAZEROUNI LAW GROUP, APC

CLASS ALLEGATIONS

68. Plaintiff brings this action on behalf of himself individually and on behalf of all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> ***All individuals whose Private Information was impacted or otherwise compromised by the Data Breach disclosed or reported by Defendants in May 2024.***

69. In addition, Plaintiff also seeks to represent a California Subclass defined as follows:

> ***All California residents whose Private Information was impacted or otherwise compromised by the Data Breach initially disclosed or reported by Defendants in May 2024.***

70. The Nationwide Class and the California Subclass are together referred to herein as the "Class."

71. Excluded from the Class are Defendants and its other subsidiaries and affiliates not named in this action; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

72. Plaintiff reserves the right to, after conducting discovery, modify, expand, or amend the above Class definition or to seek certification of a class or Classes defined differently than above before any court determines whether certification is appropriate.

73. **Numerosity.** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are thousands of members of the Class, if not more. The number of impacted individuals remains unknown and unreported, and Plaintiff believe additional entities and persons may have been affected by the Data Breach. The precise number of Class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be

KAZEROUNI LAW GROUP, APC

notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

74. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Defendants knew or should have known that their data environment and cybersecurity measures, or those created by corporate service providers, created a risk of a data breach;

b. Whether Defendants controlled and took responsibility for protecting Plaintiff's and the Class's data when they solicited that data, collected it, stored and maintained such data it on its servers, and/or authorized employees, vendors, or any third parties to access, collect, or store that data;

c. Whether Defendants' security measures were reasonable considering the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether Defendants owed Plaintiff and the Class a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected, stored, and maintained from Plaintiff and Class members;

e. Whether Defendants' failure to adequately secure Plaintiff's and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether Defendants' failure to implement reasonable data security measures allowed the breach of their data systems to occur and caused

KAZEROUNI LAW GROUP, APC

the theft of Plaintiff's and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Defendants' failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to damages and/or equitable relief and/or declaratory relief.

75. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff and the Class members are persons who provided data to Defendants, whose data was collected, stored, and maintained by Defendants and resided on Defendants' servers or systems, and whose personally identifying information was exposed in Defendants' Data Breach. Plaintiff's injuries are similar to other Class members and Plaintiff seeks relief consistent with the relief due to the Class.

76. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and committed to pursuing this matter against Defendants to obtain relief for themselves and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

77. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the

KAZEROUNI LAW GROUP, APC

class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

78. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendants, through their conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CAUSES OF ACTION

COUNT I

Negligence

79. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

80. Defendants owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited, collected, and maintained from Plaintiff and the Class. This duty arises from multiple sources.

81. Defendants owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target Defendants' data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed.

82. Defendants further knew or should have known that if hackers breached their data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, Defendants knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and

KAZEROUNI LAW GROUP, APC

the Class, was the foreseeable consequence of Defendants' unsecured, unreasonable data security measures.

83. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendants to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendants' duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendants failing to use reasonable measures to protect sensitive data. Defendants, therefore, were required and obligated to take reasonable measures to protect data they possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendants' duty to adequately protect sensitive personal information. By failing to implement reasonable data security measures, Defendants acted in violation of § 5 of the FTCA.

84. Also, the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100, imposes an affirmative duty on businesses, such as Defendants, which maintain personal information about California residents, to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendants failed to implement such procedures which resulted in the Data Breach impacting Plaintiff's and the Class members' sensitive personal information, including PII.

85. Defendants are obligated to perform their business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendants to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

86. Finally, Defendants assumed the duty to protect sensitive data by soliciting, collecting, and storing consumer data and, additionally, by representing to

KAZEROUNI LAW GROUP, APC

consumers, including its potential, former, and current customers, that it lawfully complied with data security requirements and had adequate data security measures in place to protect the confidentiality of Plaintiff's and the Class's private and sensitive personal information.

87. Defendants breached their duty to Plaintiff and the Class by implementing inadequate and/or unreasonable data security measures that they knew or should have known could cause a Data Breach. Defendants knew or should have known that hackers might target sensitive data Defendants solicited and collected, which was later collected and stored by Defendants, on customers and, therefore, needed to use reasonable data security measures to protect against a Data Breach. Indeed, Defendants acknowledged they were subject to certain standards to protect data and utilize other industry standard data security measures.

88. Defendants were fully capable of preventing the Data Breach. Defendants knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. Defendants thus failed to take reasonable measures to secure its systems, leaving Plaintiff and the Class members' sensitive personal information and/or PII vulnerable to a breach.

89. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

90. Plaintiff and the Class members have suffered damages as a result of Defendants' negligence, including actual and concrete injuries and will suffer additional injuries in the future, including economic and non-economic damages from invasion of privacy, costs related to mitigating the imminent risks of identity theft, time and effort related to mitigating present and future harms, actual identity theft, the loss of the benefit of bargained-for security practices that were not provided

KAZEROUNI LAW GROUP, APC

as represented, and the diminution of value in their Private Information and PII.

COUNT II

Negligence Per Se

91. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

92. Defendants' unreasonable data security measures constitute unfair or deceptive acts or practices in or affecting commerce in violation Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, it requires businesses to institute reasonable data security measures and breach notification procedures, which Defendants failed to do.

93. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendants of failing to use reasonable measures to protect users' sensitive data.

94. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the sensitive nature and amount of data Defendants stored on their users and the foreseeable consequences of a Data Breach should Defendants fail to secure their systems.

95. Defendants' violation of Section 5 of the FTC Act constitutes negligence per se.

96. In addition, the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100, *et seq*. requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use,

KAZEROUNI LAW GROUP, APC

modification, or disclosure." 1798.81.5(c).

97. Defendants failed to comply with the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendants failed to implement reasonable security procedures and practices to prevent an attack on its servers or systems by hackers and to prevent unauthorized access and exfiltration of Plaintiff's and Class members' PII as a result of the Data Breach.

98. Plaintiff and the Class are within the class of persons Section 5 of the FTC Act, the CCPA, and other similar state statutes, was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act. The CCPA, and other similar state statutes, was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

99. As a direct and proximate result of Defendants' negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III

Breach of Contract

100. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

101. Plaintiff and Class members entered into a valid and enforceable contract through which they were required to turn over their sensitive personal information to Defendants in exchange for services.

102. That contract included promises by Defendants to secure, safeguard, and not disclose Plaintiff's and Class members' sensitive personal information to any third parties without their consent.

KAZEROUNI LAW GROUP, APC

103. Ticketmaster's Privacy Policy published on its website[11] memorialized the rights and obligations of Defendants and its customers. This document and/or the representations contained therein was provided to Plaintiff and Class members in a manner in which it became part of the agreement for services with Defendant.

104. Aside from state and federal laws, regulations, and industry standards, through the Privacy Policy, Defendants committed to protecting the privacy and security of the sensitive personal information and promised to never share Plaintiff's and Class members' PII except under certain limited circumstances.

105. Plaintiff and Class members fully performed their obligations under their contracts with Defendant. However, Defendants failed to secure, safeguard, and/or keep private Plaintiff's and Class members' PII, and therefore Defendants breached its contracts with Plaintiff and Class members.

106. Despite Defendants' knowledge of its inadequate data security measures, Defendants continued to store and maintain possession and control of Plaintiff's and Class members' Private Information and PII, which predictably led to criminal third parties accessing and/or exfiltrating Plaintiff's and Class members' PII through Defendants' failure to reasonably safeguard such data in order to prevent the Data Breach.

107. Defendants' failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTC Act, resulted in Defendants providing services to Plaintiff and Class members that were of a diminished value and in breach of its contractual obligations to Plaintiff and Class members.

108. As a result, Plaintiff and Class members have been harmed, damaged, and/or injured as described herein, including by Defendants' failure to fully perform its part of the agreement with Plaintiff and Class members.

109. As a direct and proximate result of Defendants' conduct, Plaintiff and

[11] https://privacy.ticketmaster.com/privacy-policy

KAZEROUNI LAW GROUP, APC

Class members suffered and will continue to suffer damages in an amount to be proven at trial.

110. In addition to monetary relief, Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security monitoring and supervision procedures, conduct periodic audits of those procedures, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT IV

Breach of Implied Contract

111. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

112. Defendants provides tickets to events, as well as services related to the purchase, transfer, and sale of event tickets, to Plaintiff and Class members. Plaintiff and Class members formed an implied contract with Defendants regarding the provision of those goods and services through its collective conduct, including by Plaintiff and Class members providing their Private Information and PII to Defendants in exchange for the goods and services offered.

113. Through Defendants' offering of these goods and services, it knew or should have known that it needed to protect Plaintiff's and Class members' sensitive Private Information and PII in accordance with their own policies, practices, and applicable state and federal law.

114. As consideration, Plaintiff and Class members turned over valuable Private Information and PII relying on Defendants to securely maintain and store their Private Information and PII in return and in connection with their services.

115. Defendants accepted possession of Plaintiff's and Class members' Private Information and PII for the purpose of providing goods and services to Plaintiff and Class members.

116. In delivering their Private Information and PII to Defendants in

KAZEROUNI LAW GROUP, APC

exchange for their goods and services, Plaintiff and Class members intended and understood that Defendants would adequately safeguard their Private Information and PII as part of the goods and services which they paid Defendants for.

117. Defendants' implied promises to Plaintiff and Class members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to PII, including its business associates, vendors, and/or suppliers, also protect the confidentiality of that data; (2) taking steps to ensure that the PII that is placed in the control of its business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees, business associates, vendors, and/or suppliers; (4) designing and implementing appropriate retention policies to protect the PII against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

118. Plaintiff and Class members would not have entrusted their Private Information and PII to Defendants in the absence of such an implied contract.

119. Had Defendants disclosed to Plaintiff and the Class that they did not have adequate data security and data supervisory practices to ensure the security of their sensitive Private Information, including but not limited to Defendants' decision to continue to collect, store, and maintain Plaintiff's and Class members' Private Information and PII despite knowledge of its susceptibility to a data breach, Plaintiff and Class members would not have agreed to provide their PII to Defendant.

120. Defendants recognized (or should have recognized) that Plaintiff's and Class member's Private Information and PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the Class.

121. Defendants violated these implied contracts by failing to employ reasonable and adequate security measures and supervision of its systems and

KAZEROUNI LAW GROUP, APC

networks, as well as its vendors, business associates, and/or suppliers, to secure Plaintiff's and Class members' Private Information and PII.

122. A meeting of the minds occurred, as Plaintiff and Class members agreed, *inter alia*, to provide their accurate and complete sensitive Private Information and to Defendants in exchange for Defendants agreement to, *inter alia*, protect their Private Information and PII.

123. Plaintiff and Class members have been damaged by Defendants' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT VI

Breach of Fiduciary Duty

124. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

125. A relationship existed between Plaintiff and Class members and Defendants in which Plaintiff and Class members put their trust in Defendants to protect the Private Information and PII of Plaintiff and Class members and Defendants accepted that trust.

126. Defendants breached the fiduciary duties that they owed to Plaintiff and Class members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the Private Information and PII of Plaintiff and Class members.

127. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiff and Class members.

128. But for Defendants' breach of fiduciary duty, the damage to Plaintiff and Class members would not have occurred.

129. Defendants' breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class members.

130. As a direct and proximate result of Defendants' breach of fiduciary duty,

KAZEROUNI LAW GROUP, APC

Plaintiff is entitled to and demands actual, consequential, and nominal damages, and injunctive relief.

COUNT VII

Unjust Enrichment

131. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

132. Plaintiff and Class members conferred a benefit on Defendant. Specifically, they provided Defendants with their Private Information and PII, which has inherent value. In exchange, Plaintiff and Class members should have been entitled to Defendants' adequate protection and supervision of their Private Information and PII.

133. Defendants knew that Plaintiff and Class members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the Private Information and PII entrusted to them. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class members' P Private Information and II for business purposes.

134. Defendants failed to secure Plaintiff's and Class members' Private Information and PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their Private Information and PII provided.

135. Defendants acquired the Private Information and PII through false promises of data security and/or inequitable record retention as it failed to disclose the inadequate data security practices, procedures, and protocols previously alleged.

136. If Plaintiff and Class members had known that Defendants would not use adequate data security practices, procedures, and protocols to secure their Private Information and PII, they would have endeavored to make alternative mortgage servicing choices that excluded Defendant.

137. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred

KAZEROUNI LAW GROUP, APC

upon them.

138. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have suffered and/or will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

139. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct alleged herein. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

140. Plaintiff and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

KAZEROUNI LAW GROUP, APC

COUNT VIII

Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, et seq.
(On behalf of Plaintiff and the California Subclass)

141. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

142. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, et seq. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

143. By reason of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiff's and Class members' Private Information, Defendants engaged in unfair, unlawful, and fraudulent business practices in violation of the UCL.

144. The acts, omissions, and conduct complained of herein in violation of the UCL were designed and emanated from Defendants' California headquarters.

145. Plaintiff suffered injury, in fact, and lost money or property as a result of Defendants' alleged violations of the UCL.

146. The acts, omissions, and conduct of Defendants as alleged herein constitute a "business practice" within the meaning of the UCL.

Unlawful Prong

147. Defendants violated the unlawful prong of the UCL by violating, inter alia, the CCPA, CCRA, GLBA, and FTC Act as alleged herein.

148. Defendants violated the unlawful prong of the UCL by failing to honor the terms of its implied contracts with Plaintiff and Class Members, as alleged herein.

149. Defendants' conduct also undermines California public policy—as reflected in statutes like the California Information Practices Act, Cal. Civ. Code §§ 1798, et seq., the CCPA concerning consumer privacy, and the CCRA concerning customer records—which seek to protect customer and consumer data and ensure that

KAZEROUNI LAW GROUP, APC

entities who solicit or are entrusted with personal data utilize reasonable security measures.

Unfair Prong

150. Defendants' acts, omissions, and conduct also violate the unfair prong of the UCL because Defendants' acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other Class Members. The gravity of Defendants' conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendants' legitimate business interests, other than Defendants' conduct described herein.

151. Defendants' failure to utilize, and to disclose that it does not utilize, industry standard security practices, constitutes an unfair business practice under the UCL. Defendants' conduct is unethical, unscrupulous, and substantially injurious to the Class. While Defendants' competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Defendants have not—to the detriment of its customers and to competition.

Fraudulent Prong

152. By failing to disclose that it does not enlist industry-standard security practices, all of which rendered Class Members particularly vulnerable to data breaches, Defendants engaged in UCL-violative practices.

153. A reasonable consumer would not have transacted with Defendants if they knew the truth about its security procedures. By withholding material information about its security practices, Defendants was able to obtain customers who provided and entrusted their Personal Information in connection with transacting business with Defendant. Had Plaintiff known the truth about Defendants' security procedures, Plaintiff would not have done business with Defendant.

154. As a result of Defendants' violations of the UCL, Plaintiff and Class

KAZEROUNI LAW GROUP, APC

Members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendants utilize strong industry standard data security measures for the collection, storage, and retention of customer data; (2) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (3) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures; (5) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendants purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (7) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendants, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Private Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendants to meaningfully educate its customers about the threats they face as a result of the loss of their Private Information.

155. As a result of Defendants' violations of the UCL, Plaintiff and Class Members have suffered injury in fact and lost money or property, as detailed herein. They agreed to transact with Defendants or made purchases or spent money that they

KAZEROUNI LAW GROUP, APC

otherwise would not have made or spent, had they known the true state of affairs regarding Defendants' data security policies. Class Members lost control over their Private Information and suffered a corresponding diminution in value of that Private Information, which is a property right. Class Members lost money as a result of dealing with the fallout of and attempting to mitigate harm arising from the Data Breach.

156. Plaintiff request that the Court issue sufficient equitable relief to restore Class Members to the position they would have been in had Defendants not engaged in violations of the UCL, including by ordering restitution of all funds that Defendants may have acquired from Plaintiff and Class Members as a result of those violations.

COUNT IX

Violations of the California Consumer Legal Remedies Act (CLRA) California Civil Code §§ 1750, *et seq*. (On behalf of Plaintiff and the California Subclass)

157. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

158. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq*.

159. Defendants are the party with the most knowledge of the underlying facts giving rise to Plaintiff's allegations, so that any pre-suit notice would not put Defendants in a better position to evaluate those claims. Nevertheless, Plaintiff sent Defendants notice of claims consistent with the CLRA on or June 3, 2024.

160. To the extent the Court finds Plaintiff has still not met the CLRA notice requirements, Plaintiff in the alternative seeks only injunctive relief pursuant to Cal. Civ. Code § 1782, subdivision (d), which provides that "[a]n action for injunctive relief brought under the specific provisions of Section 1770 may be commenced without compliance with subdivision (a)."

161. Plaintiff and Class Members are "consumers," as the term is defined by

KAZEROUNI LAW GROUP, APC

California Civil Code § 1761(d).

162. Plaintiff, Class Members, and Defendants have engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

163. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct was undertaken by Defendants was likely to deceive consumers.

164. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

165. Defendants violated this provision by representing that it took appropriate measures to protect Plaintiff's and the Class Members' Private Information. Additionally, Defendants improperly handled, stored, or protected either unencrypted or partially encrypted data.

166. As a result, Plaintiff and Class Members were induced to enter into a relationship with Defendants and provide their Private Information.

167. Defendants intended to, and did, mislead Plaintiff and Class Members and induced them to rely on its misrepresentations and omissions.

168. Had Defendants disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Class Members' Private Information as part of the services Defendants provided and for which Plaintiff and Class Members paid without advising Plaintiff and Class Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Class Members' Private Information. Accordingly, Plaintiff and the Class Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

KAZEROUNI LAW GROUP, APC

169. As a result of engaging in such conduct, Defendants have violated Civil Code § 1770.

170. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks an order of this Court that includes, but is not limited to, an order enjoining Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

171. Plaintiff and Class Members suffered injuries caused by Defendants' misrepresentations, because they provided their Private Information believing that Defendants would adequately protect this information.

172. Plaintiff and Class Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

173. The unfair and deceptive acts and practices of Defendants, as described above, present a serious threat to Plaintiff and Class Members.

174. Plaintiff seeks prospective injunctive relief, including improvements to Defendants' data security systems and practices, in order to ensure that such security is reasonably sufficient to safeguard customers' Private Information that remains in Defendants' custody, including but not limited to the following:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment customer data by, among other

KAZEROUNI LAW GROUP, APC

things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants not transmit Private Information via unencrypted email;

f. Ordering that Defendants not store Private Information in email accounts;

g. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for provisions of Defendants' services;

h. Ordering that Defendants conduct regular computer system scanning and security checks;

i. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendants to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

175. Unless such Class-wide injunctive relief is issued, Plaintiff and Class Members remain at risk, and there is no other adequate remedy at law that would ensure that Plaintiff (and other consumers) can rely on Defendants' representations regarding its data security in the future.

176. Furthermore, in the alternative to all legal remedies sought herein, Plaintiff, on behalf of the Class, seeks monetary relief including but not limited to all damages recoverable under the CLRA, including, but not limited to, restitution to Plaintiff and Class Members of money or property that Defendants may have

KAZEROUNI LAW GROUP, APC

acquired by means of Defendants' unlawful, and unfair business practices; restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unlawful and unfair business practices; declaratory relief; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

COUNT X

Violations of the California Consumer Privacy Act (CCPA)
California Civil Code §§ 1798.150, *et seq*.
(On behalf of Plaintiff and the California Subclass)

177. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

178. Cal. Civ. Code § 1798.150(a) of the California Consumer Privacy Act ("CCPA") provides that "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action" for statutory damages, actual damages, injunctive relief, declaratory relief and any other relief the court deems proper.

179. Defendants violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiff and the Class. As a direct and proximate result, Plaintiff's and the Class's nonencrypted and nonredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

180. Defendants are a "business" under the meaning of Civil Code § 1798.140 because Defendants are a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the

KAZEROUNI LAW GROUP, APC

State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civil Code § 1798.140(d).

181. Plaintiff and California Subclass Members are "consumers" as defined by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in California.

182. Plaintiff and Class Members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguards Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continues to hold Private Information, including Plaintiff's and Class Members' Private Information.

183. Plaintiff and Class Members have an interest in ensuring that their Private Information is reasonably protected, and Defendants have demonstrated a pattern of failing to adequately safeguard this information.

184. On or around June 3, 2024, Plaintiff sent Defendants written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). In the event Defendants do not, or is unable to, cure the violation within 30 days, Plaintiff will amend his complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

185. Defendants failed to take sufficient and reasonable measures to safeguard its data security systems and protect Plaintiff's and California Subclass members' highly sensitive personal information and medical data from unauthorized access. Defendants' failure to maintain adequate data protections subjected Plaintiff's and the California Subclass members' nonencrypted and nonredacted sensitive personal information to exfiltration and disclosure by malevolent actors.

186. The unauthorized access, exfiltration, theft, and disclosure of Plaintiff's and the California Subclass members' Private Information was a result of Defendants' violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the

KAZEROUNI LAW GROUP, APC

personal information.

187. Under Defendants' duty to protect customers' Private Information, it was required to implement reasonable security measures to prevent and deter hackers from accessing the Private Information of its customers. These vulnerabilities existed and enabled unauthorized third parties to access and harvest customers' Private Information, evidence that Defendants have breached that duty.

188. Plaintiff and California Subclass Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

189. Defendants' violations of Cal. Civ. Code § 1798.150(a) are a direct and proximate result of the Data Breach.

190. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their PHI/Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

191. Plaintiff and the California Subclass members are further entitled to the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

192. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual damages, injunctive relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT XI

Declaratory and Injunctive Relief

193. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

KAZEROUNI LAW GROUP, APC

194. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

195. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendants' common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendants' actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

196. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed, and continue to owe a legal duty to secure the sensitive personal information with which they are entrusted, specifically including information obtained from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. Defendants breached, and continue to breach, their legal duty by failing to employ reasonable measures to secure their customers' personal information; and,

c. Defendants' breach of their legal duty continues to cause harm to Plaintiff and the Class.

197. The Court should also issue corresponding injunctive relief requiring Defendants to employ adequate security protocols consistent with industry standards to protect its users' data.

198. If an injunction is not issued, Plaintiff and the Class will suffer

KAZEROUNI LAW GROUP, APC

irreparable injury and lack an adequate legal remedy in the event of another breach of Defendants' data systems. If another breach of Defendants' data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

199. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued.

200. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themself individually and the Class, requests that this Court award judgment and relief as follows:

a. An order certifying the Class and designating Plaintiff as the Class Representative and Plaintiff's counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages and equitable relief with pre-judgment and post-judgment interest as allowed by law;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. Any other and further relief as the Court may deem necessary or appropriate.

KAZEROUNI LAW GROUP, APC

Dated: June 3, 2024

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: *s/ Abbas Kazerounian*

Abbas Kazerounian
ak@kazlg.com
Mona Amini
mona@kazlg.com
245 Fischer Avenue, Suite D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

ROBINSON CALCAGNIE, INC.
Daniel S. Robinson
drobinson@robinsonfirm.com
Michael W. Olson
molson@robinsonfirm.com
19 Corporate Plaza Drive
Newport Beach, California
Telephone: (949) 720-1288
Facsimile: (949) 720-1292

Attorneys for Plaintiff

KAZEROUNI LAW GROUP, APC

JURY TRIAL DEMANDED

Plaintiff hereby demands a jury trial for all claims and issues so triable.

Dated: June 3, 2024

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: *s/ Abbas Kazerounian*

Abbas Kazerounian
ak@kazlg.com
Mona Amini
mona@kazlg.com
245 Fischer Avenue, Suite D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

ROBINSON CALCAGNIE, INC.
Daniel S. Robinson
drobinson@robinsonfirm.com
Michael W. Olson
molson@robinsonfirm.com
19 Corporate Plaza Drive
Newport Beach, California
Telephone: (949) 720-1288
Facsimile: (949) 720-1292

Attorneys for Plaintiff

KAZEROUNI LAW GROUP, APC